

QUADRATIC POLYNOMIALS AT PRIME ARGUMENTS

JIE WU AND PING XI

ABSTRACT. For a fixed quadratic irreducible polynomial f with no fixed prime factors at prime arguments, we prove that there exist infinitely many primes p such that $f(p)$ has at most 4 prime factors, improving a classical result of Richert who requires 5 in place of 4. Denoting by $P^+(n)$ the greatest prime factor of n , it is also proved that $P^+(f(p)) > p^{0.847}$ infinitely often.

1. INTRODUCTION

It is a fundamental and challenging problem to determine in general whether a given irreducible polynomial in $\mathbf{Z}[X]$ can capture infinitely many prime values. This is known in the linear case in view of Dirichlet's theorem on primes in arithmetic progressions, but no answer is valid for any non-linear cases. A much more ambitious conjecture asserts that the above infinitude also holds if one is restricted to prime variables and there are no fixed prime factors; however, even the linear case seems beyond the current approach as predicted by the twin prime conjecture. Nevertheless, we are nowadays much heartened since $p + h$ can present infinitely many primes for certain h with $1 < |h| \leq 7 \times 10^7$, thanks to Zhang's breakthrough [Zh] on prime gaps.

In this paper, we are interested in the case of quadratic polynomials at prime arguments. It is of course beyond the current approach to prove the infinitude of primes captured by such polynomial, and alternatively, we consider the greatest prime factors and almost prime values as two approximations.

Denote by P_r the positive integers with at most r prime factors. A classical result of Richert [Ri] asserts that $f(p) = P_{2\deg f + 1}$ infinitely often for any fixed irreducible polynomial $f \in \mathbf{Z}[X]$, provided that f has no fixed prime factors at prime arguments, i.e.,

$$|\{x \pmod{p} : f(x) \equiv 0 \pmod{p}\}| < p - 1$$

for each $p \nmid f(0)$ and $p \leq \deg f + 1$. In particular, one has P_5 in the quadratic case. The progress in this direction remains blank until the recent efforts of Irving [Ir], who was able to reduce the number of prime factors while the degree is at least 3. His success comes from the application of a two-dimensional sieve which goes beyond the Bombieri-Vinogradov theorem in linear sieves. Unfortunately, his

Date: September 2, 2016.

2010 Mathematics Subject Classification. 11N32, 11N13, 11N36.

Key words and phrases. quadratic polynomial, almost prime, greatest prime factor, primes in arithmetic progressions, sieve method.

argument is not sufficient to reduce P_5 to P_4 in the quadratic case, which will be one of our aims in this paper.

Let us state our first theorem.

Theorem 1.1. *Let f be a fixed quadratic irreducible polynomial, which has no fixed prime factors at prime arguments. Then there are infinitely many primes p , such that*

$$f(p) = P_4.$$

As in [Ri], the proof also starts from the weighted sieve of Richert with logarithmic weights. To simplify the arguments, it is desirable to consider the simple case $x^2 + 1$. However, one has $2 \mid p^2 + 1$ for each odd prime p . Hence we may modify our object by taking $f(x) = \frac{1}{2}(x^2 + 1)$. In a previous joint work [WX], we are able to estimate from above the number of primes p with $p^2 + 1 \equiv 0 \pmod{q}$ for most of q , which we call *Quadratic Brun-Titchmarsh Theorem on Average*, see Lemma 2.3 below for details. This is indeed responsible for our success in the improvement to Richert's result, for which the sieve of dimension 2 can also be avoided. In fact, what we will apply for Theorem 1.1 is Lemma 2.5, which gives the birth to Lemma 2.3. Of course, in the case of an arbitrary quadratic irreducible polynomial f , one has to extend Lemma 2.5 involving the general congruence restriction $f(n) \equiv 0 \pmod{\ell}$, which can also be attacked following a similar manner together with some arguments of Lemke Oliver [LO]. One may compare Theorem 1.1 with an outstanding theorem of Iwaniec [Iw1] that $n^2 + 1 = P_2$ infinitely often.

Another approximation to prime values of $f(p)$ will be to consider the greatest prime factors. Denote by $P^+(n)$ the greatest prime factor of n .

Theorem 1.2. *Let f be a fixed quadratic irreducible polynomial. Then there are infinitely many primes p , such that*

$$P^+(f(p)) > p^{0.847}.$$

Theorem 1.2 does not require that $f(p)$ has no fixed prime factors and our proof will focus on the special case $f(x) = x^2 + 1$ to simplify the arguments. One can compare Theorem 1.2 with a celebrated theorem of Hooley [Ho] that $P^+(n^2 + 1) > n^{1.1}$ infinitely often. The first but also the last improvement is due to Deshouillers and Iwaniec [DI], for whom the exponent can be 1.202 in place of 1.1. It seems that one should require a certain strong level of distribution of primes in arithmetic progressions towards to the Elliott-Halberstam conjecture, if the exponent 0.847 in Theorem 1.2 could be replaced by some number beyond 1. The motivation of Theorem 1.2 is to restrict the variable n to sparse sets with certain multiplicative structures.

One has to mention an earlier work of Dartyge [Da], where a weaker result $P^+(p^2 + 1) > p^{0.78}$ than Theorem 1.2 was announced without proof. Of course, her interest lies in the expectation that the exponent in greatest prime factors can go beyond 1 with almost prime arguments in place of prime arguments. More

precisely, she proved, for any fixed $u > 12.2$, that there are infinitely many n , whose prime factor is at least $n^{1/u}$, such that $P^+(n^2 + 1) > n^{1+\eta}$ for some $\eta > 0$. The method (see Lemma 2.4 for details) in proving Theorem 1.2 will lead us to the following improvement, for which we only state in the case of the special polynomial $x^2 + 1$.

Theorem 1.3. *Let $u = 11.2$. Then there are infinitely many n , whose prime factor is at least $n^{1/u}$, such that*

$$P^+(n^2 + 1) > n^{1+\eta}$$

for some constant $\eta > 0$. In particular, there are infinitely many P_{11} , such that

$$P^+(P_{11}^2 + 1) > P_{11}^{1+\eta}$$

for some constant $\eta > 0$.

The paper will be organized as follows. The next section will devote to the quadratic Brun-Titchmarsh theorem and some related results on primes in arithmetic progressions, which contribute as main tools in proving Theorems 1.1 and 1.2. We will first complete the proof of Theorem 1.2 in Section 3 and the sketch for proving Theorem 1.3 will be given in Section 4. Theorem 1.1 will be proved in Section 5 after introducing the weighted sieve of Richert. The Mathematica codes can be found at <http://gr.xjtu.edu.cn/web/ping.xi/miscellanea> or requested from the authors.

Notation. Throughout this paper, γ denotes the Euler constant, letters p and q are both reserved for prime variables. A non-negative function g is defined to be smooth with compact support in $[1, 2]$ and the Fourier transform is defined by

$$\widehat{g}(\lambda) = \int_{\mathbf{R}} g(x) e^{-2\pi i \lambda x} dx.$$

Denote by φ , τ and Λ the Euler, divisor and von Mangoldt functions, respectively. The function $\rho(d)$ counts the number of incongruent solutions to the equation $a^2 + 1 \equiv 0 \pmod{d}$.

We use ε to denote an arbitrarily small positive number, which might be different at each occurrence. For a large number X , denote

$$X^{\flat} = X^{1/2} \exp(-(\log X)^{1/2}).$$

We also write $n \sim N$ for $N < n \leq 2N$.

Acknowledgements. The authors are grateful to the referee for many valuable comments. The first author is supported in part by IRT1264 from the Ministry of Education of P. R. China and the second author is supported by CPSF (No. 2015M580825) and NSF (No. 11601413) of P. R. China.

2. PRIMES IN ARITHMETIC PROGRESSIONS

2.1. Bombieri-Vinogradov Theorem. A classical result on primes in arithmetic progressions is the celebrated Bombieri-Vinogradov theorem (see [IK, Theorem 17.1] for instance). It can be stated as follows with minor modifications.

Lemma 2.1. *For any $A > 0$, we have*

$$\sum_{d \leq X^b} \tau(d)^{2016} \max_{(a,d)=1} \left| \sum_{\substack{p \geq 2 \\ p \equiv a \pmod{d}}} g\left(\frac{p}{X}\right) - \frac{1}{\varphi(d)} \sum_{p \geq 2} g\left(\frac{p}{X}\right) \right| \ll \frac{X}{(\log X)^A},$$

where the implied constant depends on A and g .

Wolke [Wo] obtained an extension of Bombieri-Vinogradov theorem replacing primes by sifted numbers without small prime factors. As an analogue of Lemma 2.1, we state the theorem of Wolke in a smoothed version. To this end, define

$$\Phi(X, z; d, a) := \sum_{\substack{n \equiv a \pmod{d} \\ p|n \Rightarrow p > z}} g\left(\frac{n}{X}\right)$$

for $(d, a) = 1$ and

$$\Phi(X, z; d) := \sum_{\substack{(n,d)=1 \\ p|n \Rightarrow p > z}} g\left(\frac{n}{X}\right).$$

Lemma 2.2. *Let $2 \leq z \leq X$. For any $A > 0$, we have*

$$\sum_{d \leq X^b} \tau(d)^{2016} \max_{(a,d)=1} \left| \Phi(X, z; d, a) - \frac{1}{\varphi(d)} \Phi(X, z; d) \right| \ll \frac{X}{(\log X)^A},$$

where the implied constant depends on A and g .

2.2. Quadratic Brun-Titchmarsh Theorem. In order to characterize primes satisfying the congruence condition $a^2 + 1 \equiv 0 \pmod{\ell}$, we consider the smoothed counting function

$$(2.1) \quad Q_\ell(X) := \sum_{\substack{p \geq 2 \\ p^2 + 1 \equiv 0 \pmod{\ell}}} g\left(\frac{p}{X}\right).$$

We proved in [WX] some upper bounds for $Q_\ell(X)$ for almost all ℓ in specialized ranges.

Lemma 2.3. *Let $A > 0$. For sufficiently large $L = X^\theta$ with $\theta \in [\frac{1}{2}, \frac{16}{17})$, the inequality*

$$(2.2) \quad Q_\ell(X) \leq \left\{ \frac{2}{\gamma(\theta)} + o(1) \right\} \widehat{g}(0) \frac{\rho(\ell)}{\varphi(\ell)} \frac{X}{\log X}$$

holds for $\ell \in (L, 2L]$ with at most $O_A(L(\log L)^{-A})$ exceptions, where

$$(2.3) \quad \gamma(\theta) := \begin{cases} \frac{91-89\theta}{62} & \text{if } \theta \in [\frac{1}{2}, \frac{64}{97}), \\ \frac{86-83\theta}{60} & \text{if } \theta \in [\frac{64}{97}, \frac{32}{41}), \\ \frac{19-18\theta}{14} & \text{if } \theta \in [\frac{32}{41}, \frac{16}{17}). \end{cases}$$

Lemma 2.3 is proved by virtue of linear sieves of Iwaniec and arithmetic exponent pairs developed in [WX]. The argument also applies to the distribution of sifted numbers in arithmetic progressions. To this end, we define

$$Q_\ell(X; u) := \sum_{\substack{n^2+1 \equiv 0 \pmod{\ell} \\ p|n \Rightarrow p > n^{1/u}}} g\left(\frac{n}{X}\right).$$

In particular, one has $Q_\ell(X) = Q_\ell(X; 2)$. In the same manner, we can prove the following theorem as an extension to Lemma 2.3.

Lemma 2.4. *Let $A > 0$. For any given $u > 0$ and sufficiently large $L = X^\theta$ with $\theta \in [\frac{1}{2}, \frac{16}{17})$, the inequality*

$$(2.4) \quad Q_\ell(X; u) \leq \{e^{-\gamma} u F(u\gamma(\theta)) + o(1)\} \widehat{g}(0) \frac{\rho(\ell)}{\varphi(\ell)} \frac{X}{\log X}$$

holds for $\ell \in (L, 2L]$ with at most $O_A(L(\log L)^{-A})$ exceptions, where $\gamma(\theta)$ is given by (2.3) and F is defined by the continuous solutions to the system

$$(2.5) \quad \begin{cases} sF(s) = 2e^\gamma & (1 \leq s \leq 2), \\ sf(s) = 0 & (0 < s \leq 2), \\ (sF(s))' = f(s-1) & (s > 2), \\ (sf(s))' = F(s-1) & (s > 2). \end{cases}$$

While applying sieve methods, one would encounter the congruence sum

$$(2.6) \quad A_d(X; \ell) := \sum_{\substack{n^2+1 \equiv 0 \pmod{\ell} \\ n \equiv 0 \pmod{d}}} g\left(\frac{n}{X}\right),$$

which is expected to be approximated by $\widehat{g}(0)\rho(\ell)(d\ell)^{-1}X$. Define

$$(2.7) \quad r_d(X; \ell) := A_d(X; \ell) - \widehat{g}(0) \frac{\rho(\ell)}{d\ell} X.$$

The following lemma characterizes the level of linear sieves and plays an essential role in proving Lemmas 2.3 and 2.4. This will also be used in the proof of Theorem 1.1.

We say that a function λ is *well-factorable of degree $J \geq 2$* , if for every decomposition $D = D_1 D_2 \cdots D_J$ with $D_1, D_2, \dots, D_J \geq 1$, there exist J arithmetic functions $\lambda_1, \lambda_2, \dots, \lambda_J$ such that

$$\lambda = \lambda_1 * \lambda_2 * \cdots * \lambda_J$$

with each λ_j of level D_j .

Lemma 2.5. *Let J be a sufficiently large integer and let λ be well-factorable of degree J . With the same notation as above, for any $\varepsilon > 0$, $\theta \in [\frac{1}{2}, \frac{112}{131})$ and $(D, L) := (X^{\eta(\theta)-\varepsilon}, X^\theta)$, there exists some $\delta = \delta(\varepsilon) > 0$ such that*

$$\sum_{\ell \sim L} \left| \sum_{d \leq D} \mu(d)^2 \lambda(d) r_d(X; \ell) \right| \ll X^{1-\delta},$$

where

$$(2.8) \quad \eta(\theta) = \frac{91 - 89\theta}{62}$$

and the implied constant depends on ε and J .

In fact, Lemma 2.5 appeared as Lemma 7.2 in [WX], where a much more delicate choice for $\eta(\theta)$ can be given in terms of (2.3). We here pick up the level (2.8) that is sharp while θ is close to $\frac{1}{2}$. It proves that this is sufficient for applications to Theorem 1.1.

3. PROOF OF THEOREM 1.2

To prove Theorem 1.2, we follow the approach of Chebyshev-Hooley, starting from the weighted sum

$$H(X) = \sum_{n \geq 1} g\left(\frac{n}{X}\right) \Lambda(n) \log(n^2 + 1).$$

Note that for $X \leq n \leq 2X$, one has

$$\log(n^2 + 1) = 2 \log n + O(1) = 2 \log X + O(1),$$

which yields

$$(3.1) \quad H(X) = \{2 \log X + O(1)\} \sum_{n \geq 1} g\left(\frac{n}{X}\right) \Lambda(n) = 2\widehat{g}(0)\{1 + o(1)\}X \log X$$

by the Prime Number Theorem. On the other hand, from the definition of Λ it follows that

$$\begin{aligned} H(X) &= \sum_{p \geq 2} g\left(\frac{p}{X}\right) (\log p) \log(p^2 + 1) + O(X^{1/2} \log X) \\ &= \{1 + o(1)\} \log X \sum_{p \geq 2} g\left(\frac{p}{X}\right) \log(p^2 + 1) + O(X^{1/2} \log X). \end{aligned}$$

Invoking the identity

$$(3.2) \quad \log(p^2 + 1) = \sum_{\ell | (p^2 + 1)} \Lambda(\ell),$$

we find

$$H(X) = \{1 + o(1)\} \log X \sum_{\ell \ll X^2} \Lambda(\ell) Q_\ell(X) + O(X^{1/2} \log X),$$

where $Q_\ell(X)$ is given by (2.1). We would like to evaluate $Q_\ell(X)$ in different ranges of ℓ . To do so, we split $H(X)$ as follows:

$$(3.3) \quad H(X) = \{1 + o(1)\} \log X \sum_{1 \leq j \leq 4} H_j(X),$$

where $\vartheta \in (\frac{1}{2}, 1)$ and

$$\begin{aligned} H_1(X) &:= \sum_{\ell \leq X^\vartheta} \Lambda(\ell) Q_\ell(X), \\ H_2(X) &:= \sum_{X^\vartheta < p \leq X^\vartheta} Q_p(X) \log p, \\ H_3(X) &:= \sum_{X^\vartheta < p \leq X^2} Q_p(X) \log p, \\ H_4(X) &:= \sum_{k \geq 2} \sum_{X^\vartheta < p^k \leq X^2} Q_{p^k}(X) \log p. \end{aligned}$$

By virtue of Lemma 2.1, one has

$$\begin{aligned} (3.4) \quad H_1(X) &= Q_1(X) \sum_{\ell \leq X^\vartheta} \frac{\Lambda(\ell) \rho(\ell)}{\varphi(\ell)} + O(X(\log X)^{-1}) \\ &= \{\tfrac{1}{2} + o(1)\} \widehat{g}(0) X. \end{aligned}$$

We now turn to consider $H_2(X)$. From Lemma 2.3 and the Prime Number Theorem, it follows that

$$H_2(X) \leq \{1 + o(1)\} \widehat{g}(0) X \int_{\frac{1}{2}}^{\vartheta} \frac{2}{\gamma(\theta)} d\theta,$$

where $\gamma(\theta)$ is given by (2.3). A numerical calculation shows that

$$\int_{\frac{1}{2}}^{\frac{64}{97}} \frac{2 \cdot 62}{91 - 89\theta} d\theta + \int_{\frac{64}{97}}^{\frac{32}{41}} \frac{2 \cdot 60}{86 - 83\theta} d\theta + \int_{\frac{32}{41}}^{\vartheta} \frac{2 \cdot 14}{19 - 18\theta} d\theta < \frac{3}{2}$$

with $\vartheta = 0.847$. This, together with (3.1), (3.3) and (3.4), implies

$$(3.5) \quad H_3(X) \gg X$$

for such ϑ , provided that

$$(3.6) \quad H_4(X) = o(X).$$

We then conclude from (3.5) that $P^+(p^2 + 1) > p^{0.847}$ for infinitely many primes p , proving Theorem 1.2.

It remains to prove (3.6) and this can be concluded from the square sieve of Heath-Brown as follows. Note, for any fixed $\ell \geq 1$, that

$$Q_\ell(X) \ll \left(\frac{X}{\ell} + 1\right) \rho(\ell),$$

from which we may derive trivially that

$$\begin{aligned} \sum_{k \geq 3} \sum_{X^b < p^k \ll X^2} Q_{p^k}(X) \log p &\ll X^\varepsilon \sum_{3 \leq k \leq 3 \log X} \sum_{X^b < p^k \ll X^2} \left(\frac{X}{p^k} + 1\right) \\ &\ll X^{1/2+\varepsilon} + X^\varepsilon \sum_{3 \leq k \leq 3 \log X} \sum_{p \ll X^{2/3}} 1 \\ &\ll X^{2/3+\varepsilon}. \end{aligned}$$

It remains to show that

$$\sum_{\sqrt{X^b} < p \ll X} Q_{p^2}(X) \log p = o(X).$$

In fact, we shall prove the following slightly stronger estimate

$$\mathcal{N}(X) := \sum_{\ell \sim L} \sum_{\substack{n \sim X \\ n^2+1 \equiv 0 \pmod{\ell^2}}} 1 \ll X^{1-\varepsilon}$$

for all $\sqrt{X^b} \ll L \ll X$. For $\sqrt{X^b} \ll L \ll X^{1-2\varepsilon}$, the above argument also applies. We only consider the remaining case $X^{1-2\varepsilon} \ll L \ll X$. In fact, the bound for $\mathcal{N}(X)$ was already obtained in [Da] appealing to the following square sieve of Heath-Brown [HB]. For the completeness of arguments, we present the proof as quickly as possible.

Lemma 3.1 (Square sieve). *Let $\xi : \mathbf{N} \rightarrow \mathbf{R}_{\geq 0}$ be an arbitrary function with $\sum_{n \in \mathbf{N}} \xi(n) < \infty$. Suppose \mathfrak{P} is a set of P prime numbers and ξ vanishes if $n = 0$ or $n \geq e^P$, then we have*

$$\sum_{n \in \mathbf{N}} \xi(n^2) \ll \frac{1}{P} \sum_{n \in \mathbf{N}} \xi(n) + \frac{1}{P^2} \sum_{p \neq q \in \mathfrak{P}} \sum_{n \in \mathbf{N}} \xi(n) \left| \sum_{n \in \mathbf{N}} \xi(n) \left(\frac{n}{pq} \right) \right|,$$

where $\left(\frac{\cdot}{pq} \right)$ denotes the Jacobi symbol $(\cdot \pmod{pq})$.

We now introduce a set \mathfrak{P} consisting of P prime numbers, where P is a large number to be specialized later. For $n^2 + 1 \equiv 0 \pmod{\ell^2}$, we can write $n^2 + 1 = m\ell^2$ for some $m \in (M, 2M]$ with $M \asymp X^2 L^{-2} \ll X^{4\varepsilon}$. Thus, we may apply the square sieve to the sequence $\{m\ell^2 - 1\}_{\ell \sim L, m \sim M}$. More precisely, we have

$$\mathcal{N}(X) \ll \frac{1}{P} \sum_{\ell \sim L} \sum_{m \sim M} 1 + \frac{1}{P^2} \sum_{\substack{p \in \mathfrak{P} \\ p \neq q}} \sum_{q \in \mathfrak{P}} \left| \sum_{\ell \sim L} \sum_{m \sim M} \left(\frac{m\ell^2 - 1}{pq} \right) \right|$$

$$\ll \frac{LM}{P} + \frac{1}{P^2} \sum_{\substack{p \in \mathfrak{P} \\ p \neq q}} \sum_{q \in \mathfrak{P}} \sum_{m \sim M} \left| \sum_{\ell \sim L} \left(\frac{m\ell^2 - 1}{pq} \right) \right|.$$

By completing method and Weil's bound for complete character sums, the innermost sum over ℓ is bounded by $(pq)^{1/2+\varepsilon}(m, pq)$. Therefore, for $X^{1-2\varepsilon} \ll L \ll X$,

$$\mathcal{N}(X) \ll LMP^{-1} + PX^{5\varepsilon} \ll X^{1-\varepsilon}$$

on taking $P = X^{5\varepsilon}$. This completes the proof of (3.6), thus that of Theorem 1.2.

4. IMPROVING A RESULT OF DARTYGE

The proof of Theorem 1.3 also follows from the Chebyshev-Hooley method. Before starting the proof, we would like to recall the counting function of sifted numbers. Write $\Phi(X, z) = \Phi(X, z; 1)$, so that

$$\Phi(X, z) := \sum_{p|n \Rightarrow p > z} g\left(\frac{n}{X}\right).$$

A classical result, $u := \log X / \log z$,

$$\Phi(X, z) = \widehat{g}(0) \frac{Xw(u) - z}{\log z} + O\left(\frac{X}{(\log z)^2}\right),$$

where $w(u)$ is the Buchstab function defined recursively by

$$\begin{cases} uw(u) = 1 & (1 \leq u \leq 2), \\ (uw(u))' = w(u-1) & (u > 2). \end{cases}$$

Suppose now $1 < u \leq 13$, and we would like to examine the sum

$$H(u, X) := \sum_{p|n \Rightarrow p > X^{1/u}} g\left(\frac{n}{X}\right) \log(n^2 + 1).$$

On one hand, we have

$$H(u, X) = \{2 \log X + O(1)\} \Phi(X, X^{1/u}) = 2uw(u) \widehat{g}(0) X \{1 + o(1)\}.$$

On the other hand, the relation (3.2) allows us to write

$$H(u, X) = \sum_{\ell \ll X^2} \Lambda(\ell) \sum_{\substack{p|n \Rightarrow p > X^{1/u} \\ n^2 + 1 \equiv 0 \pmod{\ell}}} g\left(\frac{n}{X}\right) = \sum_{\ell \ll X^2} \Lambda(\ell) Q_\ell(X; u)$$

and split the sum over ℓ following the manner in (3.3). By virtue of Lemmas 2.2 and 2.4, it suffices to find the smallest $u > 1$ such that

$$\int_{\frac{1}{2}}^{\frac{16}{17}} F(u\gamma(\theta)) d\theta + \int_{\frac{16}{17}}^{\theta_0} F(u(1-\theta)) d\theta + \frac{u}{e^\gamma} \int_{\theta_0}^1 \frac{\theta d\theta}{\sigma_2\left(\left(\frac{2}{3} - \frac{\theta}{2}\right)u\right)} < \frac{3}{2} e^\gamma w(u),$$

where $\theta_0 = 0.9926$ as chosen in [Da, Section 9], $\gamma(\theta)$ is given by (2.3), the second integral comes from the classical Brun-Titchmarsh theorem of van Lint-Richert and $1/\sigma_2(s)$ appears in the Selberg sieve of dimension 2, which is equal to $8e^{2\gamma}s^{-2}$ if $0 < s \leq 2$. One may check with the help of Mathematica 9 that $u = 11.2$ works.

5. PROOF OF THEOREM 1.1

5.1. Preparation for sifting. We first state some convention to sift the specialized sequence

$$\mathcal{A} := \left\{ \frac{1}{2}(p^2 + 1) : X < p \leq 2X \right\},$$

although most arguments are suited for all general non-negative sequences.

Define the *smoothed* sifting function

$$S(\mathcal{A}, z) := \sum_{(\frac{1}{2}(p^2+1), P(z))=1} g\left(\frac{p}{X}\right),$$

where, for $z > 3$,

$$P(z) := \prod_{2 < p < z} p.$$

For squarefree d , we consider subsequence

$$\mathcal{A}_d := \left\{ \frac{1}{2}(p^2 + 1) : X < p \leq 2X \text{ and } p^2 + 1 \equiv 0 \pmod{d} \right\}.$$

Its sifting function is defined by

$$S(\mathcal{A}_d, z) = \sum_{\substack{(\frac{1}{2}(p^2+1), P(z))=1 \\ p^2+1 \equiv 0 \pmod{d}}} g\left(\frac{p}{X}\right).$$

Recall congruence sum $Q_d(X)$, defined by (2.1). For $d \leq X^b$, the Bombieri-Vinogradov theorem (see Lemma 2.1) yields that $Q_d(X)$ can be approximated on average by $Q_1(X)\rho(d)/\varphi(d)$.

The following lemma then characterizes the dimension of sieves, see [DH, Proposition 10.1] for instance.

Lemma 5.1. *For $z > 3$, we have*

$$(5.1) \quad \sum_{p \leq z} \frac{\rho(p)}{\varphi(p)} \log p = \log z + O(1)$$

and

$$(5.2) \quad V(z) := \prod_{2 < p \leq z} \left(1 - \frac{\rho(p)}{\varphi(p)} \right) = \{1 + o(1)\} \frac{e^{-\gamma} \mathfrak{c}}{\log z}$$

with

$$\mathfrak{c} := 2 \prod_{p>2} \left(1 - \frac{\rho(p)}{\varphi(p)}\right) \left(1 - \frac{1}{p}\right)^{-1}.$$

5.2. A weighted sieve. We now introduce the weighted sieve of Richert following the manner in [Ri]. Let $0 < \alpha < \beta$ be some constants to be specialized later. Put

$$z := X^\alpha, \quad y := X^\beta, \quad \eta := r + 1 - 2/\beta.$$

Consider the weighted sum

$$\Psi(\alpha, \beta; \eta) := \sum_{(\frac{1}{2}(p^2+1), P(z))=1} g\left(\frac{p}{X}\right) \left(1 - \frac{1}{\eta} \sum_{\substack{q|(p^2+1) \\ z \leq q < y}} w_q\right)$$

with $w_q := 1 - (\log q)/\log y$. Note that q is a prime variable.

The following lemma is taken from [Ri] with slight modification in notation.

Lemma 5.2. *Suppose that for a given $r \geq 1$, there exist constants α, β with*

$$0 < \alpha < \beta < 1, \quad \beta > 2/(r+1)$$

such that

$$(5.3) \quad \Psi(\alpha, \beta; \eta) \gg X(\log X)^{-2}.$$

Then we have

$$|\{X < p \leq 2X : \tfrac{1}{2}(p^2+1) = P_r\}| \gg X(\log X)^{-2}.$$

Theorem 1.1, in the case of such special polynomial, follows from suitable choices for α, β such that (5.3) holds with $r = 4$. To do so, we will seek the lower bound for $\Phi(\alpha, \beta; \eta)$ starting from the following expression

$$(5.4) \quad \Psi(\alpha, \beta; \eta) = S(\mathcal{A}, z) - \eta^{-1} \sum_{z \leq q < y} w_q S(\mathcal{A}_q, z).$$

5.3. Sieve estimates. The lower bound for $S(\mathcal{A}, z)$ follows from a routine application of lower-bound sieve and Lemma 2.1.

Lemma 5.3. *For $X \rightarrow +\infty$, we have*

$$S(\mathcal{A}, z) \geq f\left(\frac{1}{2\alpha}\right) \widehat{g}(0) V(z) \frac{X}{\log X} \{1 + o(1)\},$$

where f is defined by the system (2.5) and $V(z)$ is given by (5.2).

An upper bound for $S(\mathcal{A}_q, z)$ with small primes q follows from the upper-bound sieve and Lemma 2.1. For larger primes q , especially while going beyond the Bombieri-Vinogradov theorem, we will appeal to Lemma 2.5 combining with a composition of two linear sieves. To do so, we introduce a parameter $\delta \in (\alpha, \beta)$ to be optimized.

Lemma 5.4. *For $X \rightarrow +\infty$, we have*

$$\sum_{z \leq q < X^\delta} w_q S(\mathcal{A}_q, z) \leq c_1 \widehat{g}(0) V(z) \frac{X}{\log X} \{1 + o(1)\},$$

where $V(z)$ is given by (5.2) and

$$(5.5) \quad c_1 := \int_\alpha^\delta \left(\frac{1}{\theta} - \frac{1}{\beta} \right) F\left(\frac{1-2\theta}{2\alpha} \right) d\theta.$$

Proof. In fact, an upper-bound sieve of Rosser-Iwaniec yields

$$\begin{aligned} S(\mathcal{A}_q, z) &\leq \frac{X}{\log X} \widehat{g}(0) V(z) \frac{\rho(q)}{\varphi(q)} \left\{ F\left(\frac{\log(X^\flat/q)}{\log z} \right) + O\left(\frac{1}{(\log X)^{1/6}} \right) \right\} \\ &\quad + O\left(\sum_{d \leq X^\flat/q} \left| Q_{qd}(X) - \frac{\rho(qd)}{\varphi(qd)} Q_1(X) \right| \right), \end{aligned}$$

where F is defined recursively by (2.5). Summing over q against the weight w_q with integration by parts thanks to (5.1) and controlling the error term by virtue of Lemma 2.1, we get the required result. \square

We now turn to consider $S(\mathcal{A}_q, z)$ for $q \geq X^\delta$. We will appeal to Lemma 2.5 instead of Lemma 2.1.

Lemma 5.5. *Let $\beta < 0.68$. For $X \rightarrow +\infty$, we have*

$$\sum_{X^\delta \leq q < X^\beta} w_q S(\mathcal{A}_q, z) \leq c_2 \widehat{g}(0) V(z) \frac{X}{\log X} \{1 + o(1)\},$$

where

$$(5.6) \quad c_2 := e^\gamma \alpha \int_\delta^\beta \left(\frac{1}{\theta} - \frac{1}{\beta} \right) \frac{88288 d\theta}{8281 - 16198\theta + 7921\theta^2}.$$

Proof. We would like to make initial estimates for each $S(\mathcal{A}_q, z)$ from above by the composition of two upper-bound linear sieves (see Theorem A.1 below), and then all parameters will be optimized after summing over q .

For $Q = X^\theta$ with $\delta \leq \theta \leq \beta$, define

$$\mathcal{C}(Q) := \sum_{Q < q \leq 2Q} w_q S(\mathcal{A}_q, z).$$

Let λ_1, λ_2 be two upper-bound linear sieves, of level D_1, D_2 , so that $0 \leq 1 * \mu \leq 1 * \lambda_i$ for $i = 1, 2$. We thus have, with $P_* = \prod_{p \leq \sqrt{X}} p$ and the notation (2.6),

$$S(\mathcal{A}_q, z) = \sum_{d_1 | P(z)} \mu(d_1) \sum_{\substack{d_2 | P_* \\ (d_2, qd_1) = 1}} \mu(d_2) A_{d_2}(X; 2d_1q)$$

$$\leq \sum_{\substack{d_1 \leq D_1 \\ d_1 | P(z)}} \sum_{\substack{d_2 \leq D_2 \\ (d_2, qd_1)=1}} \lambda_1(d_1) \lambda_2(d_2) A_{d_2}(X; 2d_1q).$$

The conditions that $d_1 | P(z)$ and $q \geq z$ implies that $(d_1, q) = 1$. Replacing $A_{d_2}(X; 2d_1q)$ by $\widehat{g}(0)\rho(d_1)\rho(q)(d_1d_2q)^{-1}X + r_{d_2}(X; 2qd_1)$ (cf. (2.7)) and inserting the obtained inequality into the definition of $\mathcal{C}(Q)$, we find that

$$(5.7) \quad \mathcal{C}(Q) \leq \mathcal{M}(Q) + \mathcal{E}(Q)$$

with

$$\begin{aligned} \mathcal{M}(Q) &:= \widehat{g}(0)X \sum_{Q < q \leq 2Q} w_q \frac{\rho(q)}{q} \sum_{\substack{d_1 \leq D_1 \\ d_1 | P(z)}} \frac{\lambda_1(d_1)\rho(d_1)}{d_1} \sum_{\substack{d_2 \leq D_2 \\ (d_2, qd_1)=1}} \frac{\lambda_2(d_2)}{d_2}, \\ \mathcal{E}(Q) &:= \sum_{Q < q \leq 2Q} w_q \sum_{\substack{d_1 \leq D_1 \\ d_1 | P(z)}} \sum_{\substack{d_2 \leq D_2 \\ (d_2, qd_1)=1}} \lambda_1(d_1) \lambda_2(d_2) r_{d_2}(X; 2qd_1). \end{aligned}$$

Thanks to Iwaniec [Iw2], the sieve weights λ_1, λ_2 can be chosen to be finite linear combinations of some functions that are well-factorable of degree J for any fixed large $J \geq 2$, so that we are in a position to apply Lemma 2.5, getting

$$(5.8) \quad \mathcal{E}(Q) \ll X^{1-\delta}$$

for some $\delta > 0$, provided that

$$(5.9) \quad \gamma_2 < \frac{91}{62} - \frac{89}{62}(\gamma_1 + \theta), \quad \frac{1}{2} \leq \gamma_1 + \theta < \frac{112}{131}$$

with

$$D_1 = X^{\gamma_1}, \quad D_2 = X^{\gamma_2}, \quad Q = X^\theta.$$

The upper bound for $\mathcal{C}(Q)$ will be established by evaluating the main term $\mathcal{M}(Q)$. This is in fact a composition of two linear upper-bound sieves, and we appeal to a reduction of Friedlander and Iwaniec, see Theorem A.1 in the appendix, in which we should take

$$g_1(d) = \begin{cases} \rho(d)/d & (2 \nmid d) \\ 0 & (2 \mid d) \end{cases} \quad \text{and} \quad g_2(d) = \begin{cases} 1/d & (q \nmid d) \\ 0 & (q \mid d) \end{cases}.$$

It is easy to check that both of g_1, g_2 satisfy the restriction (A.1). Hence it follows

$$(5.10) \quad \mathcal{M}(Q) \leq \{1 + o(1)\} \widehat{g}(0) \frac{4e^\gamma \alpha}{\mathfrak{c} \gamma_1 \gamma_2} \frac{XV(z)}{\log X} \sum_{Q < q \leq 2Q} w_q \frac{\rho(q)}{q} H_q,$$

where \mathfrak{c} is defined in Lemma 5.1 and H_q corresponds to H in Theorem A.1 upon the above choices for g_1, g_2 , i.e.,

$$H_q = 2 \left(1 - \frac{\rho(q)}{q}\right) \left(1 - \frac{1}{q}\right)^{-2} \prod_{p \nmid 2q} \left(1 - \frac{1 + \rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-2}$$

$$= 2 \left(1 - \frac{\rho(q)}{q}\right) \left(1 - \frac{1 + \rho(q)}{q}\right)^{-1} \prod_{p>2} \left(1 - \frac{1 + \rho(p)}{p}\right) \left(1 - \frac{1}{p}\right)^{-2},$$

which can be reduced to

$$H_q = \mathfrak{c} \cdot \left(1 - \frac{\rho(q)}{q}\right) \left(1 - \frac{1 + \rho(q)}{q}\right)^{-1}$$

since $\rho(p) = 2$ for $p \equiv 1 \pmod{4}$ and $\rho(p) = 0$ for $p \equiv 3 \pmod{4}$.

It suffices to maximize $\gamma_1 \gamma_2$, in terms of θ , subject to the constraints in (5.9). With the help of Mathematica 9, we have

$$\gamma_1 \gamma_2 < \frac{1}{22072} (8281 - 16198\theta + 7921\theta^2) \quad \text{for } \theta \in (0, \frac{8015}{11659}).$$

One may see why we require $\beta < 0.68 < \frac{8015}{11659}$ in Lemma 5.5.

Collecting all Q , Lemma 5.5 then follows from (5.7), (5.8), (5.10) and partial summation. \square

5.4. Conclusion of Theorem 1.1. We conclude from Lemmas 5.3-5.5 that

$$(5.11) \quad \Psi(\alpha, \beta; \eta) \geq C \widehat{g}(0) V(z) \frac{X}{\log X} \{1 + o(1)\}$$

with

$$C := f\left(\frac{1}{2\alpha}\right) - \frac{1}{\eta} \int_{\alpha}^{\delta} \left(\frac{1}{\theta} - \frac{1}{\beta}\right) F\left(\frac{1-2\theta}{2\alpha}\right) d\theta \\ - \frac{e^{\gamma}\alpha}{\eta} \int_{\delta}^{\beta} \left(\frac{1}{\theta} - \frac{1}{\beta}\right) \frac{88288 d\theta}{8281 - 16198\theta + 7921\theta^2}.$$

For $\theta \geq \frac{1}{2} - 3\alpha$, we find

$$F\left(\frac{1-2\theta}{2\alpha}\right) = \frac{4e^{\gamma}\alpha}{1-2\theta}.$$

Thus, $\delta \approx 0.44$ is chosen to be the root of the equation

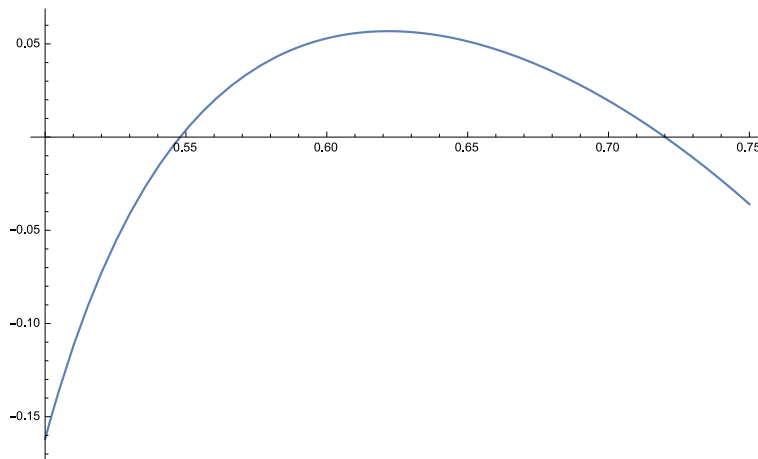
$$\frac{1}{1-2\delta} = \frac{22072}{8281 - 16198\delta + 7921\delta^2}.$$

We choose $\alpha = \frac{1}{12}$, so that

$$\frac{1-2\theta}{2\alpha} = 6(1-2\theta) \in \begin{cases} [1, 3] & \text{if } \theta \in [\frac{1}{4}, \delta], \\ [3, 5] & \text{if } \theta \in [\frac{1}{12}, \frac{1}{4}]. \end{cases}$$

Note that

$$F(s) = \begin{cases} \frac{2e^{\gamma}}{s} & (1 \leq s \leq 3), \\ \frac{2e^{\gamma}}{s} \left(1 + \int_2^{s-1} \frac{\log(t-1)}{t} dt\right) & (3 \leq s \leq 5). \end{cases}$$


 FIGURE 1. Graph for $C = C(\beta)$ with $r = 4$

This will lead to the following more explicit expression for C

$$C = f(6) - \frac{e^\gamma}{3\eta} \left\{ \int_{\frac{1}{12}}^{\frac{1}{4}} \left(\frac{1}{\theta} - \frac{1}{\beta} \right) \left(1 + \int_2^{6(1-2\theta)^{-1}} \frac{\log(t-1)}{t} dt \right) \frac{d\theta}{1-2\theta} \right. \\ \left. + \int_{\frac{1}{4}}^{0.44} \left(\frac{1}{\theta} - \frac{1}{\beta} \right) \frac{d\theta}{1-2\theta} + \int_{0.44}^{\beta} \left(\frac{1}{\theta} - \frac{1}{\beta} \right) \frac{22072 d\theta}{8281 - 16198\theta + 7921\theta^2} \right\}.$$

Taking $r = 4$ and $\beta = 0.622$, we find $C \approx 0.0568$. This establishes Theorem 1.1 in view of Lemma 5.2.

APPENDIX A. COMPOSITION OF TWO LINEAR SIEVES

In this appendix, we formulate a reduction of Friedlander and Iwaniec on the composition of two sieves. In particular, we focus on linear sieves. The original statement with proof can be found in [FI1, Appendix A] or [FI2, Section 5.10].

Theorem A.1. *Let (λ_1) , (λ_2) be two upper-bound linear sieves of levels D_1, D_2 , respectively, and let g_1, g_2 be density functions satisfying linear sieve conditions and*

$$(A.1) \quad 0 \leq g_1(p), g_2(p) \leq \frac{1}{2}$$

for each prime p . Then

$$\left| \sum_{(d_1, d_2)=1} \lambda_1(d_1) \lambda_2(d_2) g_1(d_1) g_2(d_2) \right| \leq \frac{4H \{1 + o(1)\}}{\log D_1 \log D_2}$$

with

$$H := \prod_p (1 - g_1(p) - g_2(p))(1 - 1/p)^{-2}.$$

One can see that we have an extra condition (A.1) compared to the original version of Friedlander and Iwaniec, for whom the constant H should be replaced by the following larger one

$$\prod_p (1 - g_1(p) - g_2(p) + 2g_1(p)g_2(p))(1 - 1/p)^{-2}.$$

The modification here is due to avoiding the use of the trivial inequality

$$\left| 1 - \frac{g_1 g_2}{(1 - g_1)(1 - g_2)} \right| \leq 1 + \frac{g_1 g_2}{(1 - g_1)(1 - g_2)}$$

at primes.

REFERENCES

- [Da] C. Dartyge, Le plus grand facteur premier de $n^2 + 1$ où n est presque premier, *Acta Arith.* **LXXVI.3** (1996), 199–226.
- [DI] J.-M. Deshouillers & H. Iwaniec, On the greatest prime factor of $n^2 + 1$, *Ann. Inst. Fourier (Grenoble)* **32** (1982), 1–11.
- [DH] H. G. Diamond & H. Halberstam, A Higher-Dimensional Sieve Method, Cambridge Tracts in Math. **177**, Cambridge Univ. Press, Cambridge, 2008.
- [FI1] J. B. Friedlander & H. Iwaniec, Hyperbolic prime number theorem, *Acta Math.* **202** (2009), 1–19.
- [FI2] J. B. Friedlander & H. Iwaniec, Opera de Cribro, *Amer. Math. Soc. Colloq. Publ.*, Vol. **57**, AMS, Providence, RI, 2010.
- [HB] D. R. Heath-Brown, The square sieve and consecutive square-free numbers, *Math. Ann.* **266** (1984), 251–259.
- [Ho] C. Hooley, On the greatest prime factor of a quadratic polynomial, *Acta Math.* **117** (1967), 281–299.
- [Ir] A. J. Irving, Almost-prime values of polynomials at prime arguments, *Bull. London Math. Soc.* **47** (2015), 593–606.
- [Iw1] H. Iwaniec, Almost-primes represented by quadratic polynomials, *Invent. Math.* **47** (1978), 171–188.
- [Iw2] H. Iwaniec, A new form of the error term in the linear sieve, *Acta Arith.* **37** (1980), 307–320.
- [IK] H. Iwaniec & E. Kowalski, Analytic Number Theory, *Amer. Math. Soc. Colloq. Publ.*, Vol. 53, AMS, Providence, RI, 2004.
- [LO] R. J. Lemke Oliver, Almost-primes represented by quadratic polynomials, *Acta Arith.*, **151** (2012), 241–261.
- [Ri] H.-E. Richert, Selberg’s sieve with weights, *Mathematika* **16** (1969), 1–22.
- [Wo] D. Wolke, Über die mittlere Verteilung der Werte zahlentheoretischer Funktionen auf Restklassen. II, *Math. Ann.* **204** (1973), 145–153.
- [WX] J. Wu & P. Xi, Arithmetic exponent pairs for algebraic trace functions and applications, arXiv:1603.07060 [math.NT]
- [Zh] Y. Zhang, Bounded gaps between primes, *Ann. of Math. (2)* **179** (2014), 1121–1174.

SCHOOL OF MATHEMATICS, SHANDONG UNIVERSITY, JINAN, SHANDONG 250100, P. R.
CHINA

E-mail address: `jie.wu@univ-lorraine.fr`

DEPARTMENT OF MATHEMATICS, XI'AN JIAOTONG UNIVERSITY, XI'AN 710049, P. R.
CHINA

E-mail address: `ping.xi@xjtu.edu.cn`